Certifying entangled measurements in known Hilbert spaces

Tamás Vértesi[1] and Miguel Navascués[2]

[1]Institute of Nuclear Research of the Hungarian Academy of Sciences
[2]Facultad de Matemáticas, Universidad Complutense de Madrid

We study under which conditions it is possible to assert that a joint demolition measurement cannot be simulated by Local Operations and Classical Communication. More concretely, we consider a scenario where two parties, Alice and Bob, send each an unknown state to a third party, Charlie, who in turn interacts with the states in some undisclosed way and then announces an outcome. We show that, under the assumption that Alice and Bob know the dimensionality of their systems, there exist situations where the statistics of the outcomes reveals the nature of Charlie's measurement.

I. INTRODUCTION

Quantum nonlocality, the fact that entangled quantum systems separated in space can violate Bell inequalities [1], is one of the most profound discoveries in science. This nonlocal nature of entanglement has also been identified as an essential resource for various quantum information processing tasks. It allows to reduce communication complexity [2] or makes it possible to devise device-independent protocols for quantum key distribution [3], genuine random number generations [4], and state tomography [5]. Indeed, these tasks can be performed without resorting to the actual inner working of the devices, which is a feat without counterpart in the classical world.

In all of the above instances, quantum nonlocality arises when space-like separated measurements are performed over jointly prepared entangled states. However, the existence of nonlocality can also be manifested in a dual setup [6],[7]: quantum states which are prepared separately (hence unentangled) exhibit anomalous correlations when measured jointly. In this case, more information can be revealed by joint measurements than can be gained by using any sequence of Local Operations assisted by Classical Communication (LOCC). In particular, the superiority of globally entangled measurements over LOCC ones has been proved conclusively [8]. The improved performance is due to entanglement occurring in the process of measurement and again it is not associated with the states.

For quantifying the effectiveness of entangled measurements, different figures of merit have been proposed, like the Shannon mutual information [6] or the quantum fidelity [8]. A common feature of those is, though, that one must rely both on the precise *form of the states* prepared and on the *a priori probabilities* of the preparations; otherwise, the estimations on the figure of merit would be not reliable. Hence, in order to ascertain that a measurement is truly globally entangled and not only an LOCC one, one must resort to a detailed knowledge of the preparation procedure. Clearly, this issue sheds doubt on the reliability of the obtained results.

In the present paper we take another approach, more in the spirit of a black box scenario, and tackle the problem of certifying entangled measurements by introducing a kind of dual Bell inequalities. These inequalities involve correlation terms which can be gathered from experimental data, and do not depend on the specific form of the quantum states to be prepared. Actually, the only necessary condition entering in the derivation is the Hilbert space dimension of the prepared particles. Taking into account that entangled measurements enable increased classical capacity of quantum channels [9] and efficient quantum state estimation [10], in the future it would also be interesting to find applications related to these tasks within a black box approach.

The notation we use along the article is introduced in the next section. Section III provides an instance of certifiable entangled measurements based on a nonlinear inequality. Section IV is devoted to a numerical study where linear inequalities are applied to detect entangled measurements in the simplest possible scenarios. Section V summarizes our conclusions.

II. PRELIMINARIES AND NOTATION

Let us imagine the following communication scenario, close to the spirit of the simultaneous message passing model [11]. Two separated parties, Alice and Bob, have each some preparation device with N possible inputs. Alice (Bob) is thus able to prepare any of the unknown qudit states $\{\rho_x \in \mathbb{C}^D\}_{x=1}^N$ ($\{\sigma_y \in \mathbb{C}^D\}_{y=1}^N$). Alice and Bob then send their states to a third party, Charlie, who performs a measurement over those two states, announcing a dit a of dimension K at the end of the process. Denote by $\{M_a : a = 0, ..., K-1\}$ the elements of Charlie's Positive Operator Valued Measure (POVM). Then, for each pair of inputs x and y, several repetitions of this primitive would allow Alice and Bob to estimate the frequency of occurrence

$$P(a|x,y) \equiv \text{tr}(\rho_x \otimes \sigma_y \cdot M_a) \qquad (1)$$

of each outcome $a = 1, 2, \ldots, K$. Depending on the form of the POVM elements $\{M_a : a = 0, ..., K-1\}$, we will distinguish four different types of measurements:

Classical measurements. Suppose that Charlie's measurement is fixed in advance to a given complete projective measurement on each system (say, in the computational basis), followed by some random processing
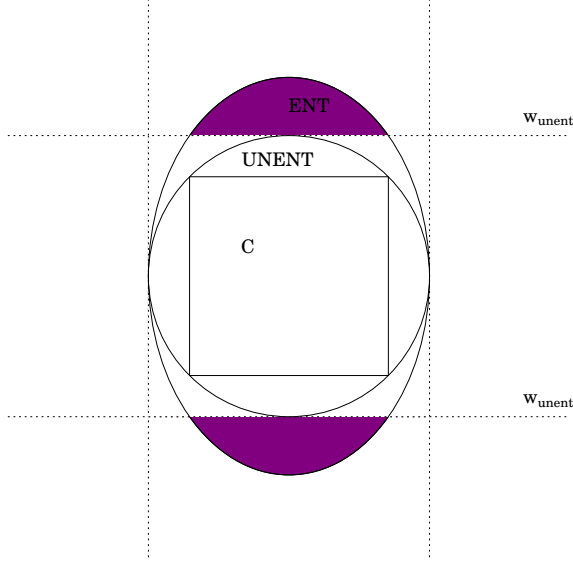
FIG. 1: A schematic picture of the 2-dimensional slice of the probability space for different sets in the general NDK scenario. The square represents the classical set P^C, the circle and the ellipse designate the set of unentangled (P^{unent}) and the set of entangled measurements (P^{ent}), respectively. In the purple region entangled measurements are witnessed by linear inequalities.

of the raw output. Any set of distributions $P(a|x,y)$ so generated can be reproduced in a classical setting where Alice and Bob send each one dit of information to Charlie, who, in turn, applies a random function $f : \{0, ..., D-1\} \times \{0, ..., D-1\} \to K$ and then announces the result. For each NDK scenario, we will denote by $\tilde{P}^C$ the set of all possible correlations $P(a|x,y)$ that can be attained in such a way.

It is easy to see that any point of $\tilde{P}^C$ is a convex combination of deterministic classical strategies. As we will see, though, the converse is not true. On the other hand, if Alice, Bob and Charlie share random variables, then any convex sum of deterministic strategies can be attained. Since for any NDK scenario the number of deterministic classical strategies is finite, the set of correlations attainable through classical maps and shared randomness is a polytope, that we will denote by P^C. This classical set is symbolized in Figure 1 by a square.

Unentangled and LOCC measurements. If each of the POVM elements M_a is a separable operator, we will say that the measurement M is unentangled. We will say that Charlie's measurement can be attained via Local Operations and Classical Communications (LOCC) if M corresponds to a sequence of local measurements on Alice's and Bob's individual qubits, with each measurement possibly depending on the outcomes of earlier measurements. It is known that the class of unentangled measurements is strictly greater than the class of LOCC measurements [7]. This implies that $\tilde{P}^{unent} \supseteq \tilde{P}^{LOCC}$,

where $\tilde{P}^{unent}, \tilde{P}^{LOCC}$ resp. denote the sets of distributions $P(a|x,y)$ attainable through unentangled and LOCC measurements in a given NDK scenario. It is an open question whether such an inclusion is strict.

As before, if we allow Alice, Bob and Charlie share some prior random variables, the resulting sets of correlations $P^{unent} \supseteq P^{LOCC}$ are convexifications of the former. A two-dimensional slice of the unentangled set P^{unent} is symbolized in Figure 1 by a circle.

General measurements. Here the measurement operators are only limited by positivity and normalization constraints, i.e.,

$$M_a \succeq 0, \quad \sum_{a=0}^{K-1} M_a = \mathbb{I}, \tag{2}$$

where the operators $M_a \in B(\mathbb{C}^D \otimes \mathbb{C}^D)$ may very well be entangled. These are the most general measurements allowed by quantum mechanics. In analogy with the former sets, we will denote by $\tilde{P}^{ent}$ and P^{ent} the set of distributions accessible through general joint measurements and its convex hull. The latter is depicted as an ellipse in Figure 1.

The numerical study of the sets $\tilde{P}^C$, $\tilde{P}^{unent}$ and $\tilde{P}^{ent}$ is much more convoluted than that of their convexifications P^C, P^{unent} and P^{ent}. Consequently, most of this article is devoted to the numerical analysis of the latter.

If we reflex a bit about the previous definitions, it will soon be clear that the above sets of correlations can only be distinguished experimentally in a black box way if the NDK scenario is such that $N > D$. Otherwise, by forcing Alice and Bob to send orthogonal states, Charlie could always infer the values of x, y through an appropriate projective measurement, and so *any* conceivable distribution $P(a|x,y)$ could be classically realized. The simplest scenario where we may expect to find an interesting structure is thus the 322 scenario. And, indeed, the next example shows that there the sets $\tilde{P}^C$ and $\tilde{P}^{unent}$ differ from $\tilde{P}^{ent}$. It also proves that neither of the former two sets is convex, and so the convexifications P^C, P^{LOCC}, P^{unent} are non-trivial.

III. AN INSTANCE OF ENTANGLEMENT DETECTION

Consider the 322 scenario, and denote by P the matrix of probabilities $P_{xy} \equiv P(0|x,y)$. Suppose now that

$$P = \begin{pmatrix} 0 & 1/4 & 1/4 \\ 1/4 & 0 & 1/4 \\ 1/4 & 1/4 & 0 \end{pmatrix}. \tag{3}$$

This set of probabilities can be attained if the states $\{\rho_x, \sigma_y\}$ and the POVM element $M \equiv M_{a=0}$ correspond

to

$$\rho_1 = |0\rangle\langle 0|, \quad \rho_2 = |+\rangle\langle +|, \quad \rho_3 = |+i\rangle\langle +i|,$$
$$\sigma_1 = |1\rangle\langle 1|, \quad \sigma_2 = |-\rangle\langle -|, \quad \sigma_3 = |+i\rangle\langle +i|, \quad (4)$$

$$M = |\Psi^+\rangle\langle\Psi^+|, \quad (5)$$

where $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. It hence follows that $P \in \tilde{P}^{ent}$.

We will prove that M must be an entangling measure (i.e., $P \notin \tilde{P}^{unent}$) by *reductio ad absurdum*. Imagine, therefore, that M is separable, i.e., $M = \sum_{i=1}^K \lambda_i |u_i\rangle\langle u_i| \otimes |v_i\rangle\langle v_i|$. Then, the condition $P_{11} = 0$ implies that: 1) ρ_1 or σ_1 (or both) is a pure quantum state; and 2) there exists a subset of indices $\mathcal{I} \subset \{1, 2, ..., K\}$ such that

$$M = \sum_{i\in\mathcal{I}} \lambda_i \rho_1^\perp \otimes |v_i\rangle\langle v_i| + \sum_{i\notin\mathcal{I}} \lambda_i |u_i\rangle\langle u_i| \otimes \sigma_1^\perp. \quad (6)$$

Here $\omega^\perp$ denotes $\mathbb{I}_2 - \omega^\perp$, for any qubit state ω. From $\text{tr}(M\rho_1 \otimes \sigma_1) = P_{11} \neq P_{12} = \text{tr}(M\rho_1 \otimes \sigma_2)$ we have that $\sigma_1 \neq \sigma_2$, and thus $\text{tr}(\sigma_1\sigma_2^\perp) \neq 0$. Likewise, $\text{tr}(\rho_x\rho_{x'}^\perp), \text{tr}(\sigma_y\sigma_{y'}^\perp) \neq 0$, for all $y \neq y', x \neq x'$. This implies that

$$\text{tr}(M\rho_2 \otimes \sigma_2) = \sum_{i\in\mathcal{I}} \lambda_i \text{tr}(\rho_1^\perp \rho_2)\text{tr}(|v_i\rangle\langle v_i|\sigma_2)$$
$$+ \sum_{i\notin\mathcal{I}} \lambda_i \text{tr}(|u_i\rangle\langle u_i|\rho_2)\text{tr}(\sigma_1^\perp \sigma_2)$$
$$\geq \delta \sum_{i\in\mathcal{I}} \lambda_i \text{tr}(|v_i\rangle\langle v_i|\sigma_2) + \delta \sum_{i\notin\mathcal{I}} \lambda_i \text{tr}(|u_i\rangle\langle u_i|\rho_2), \quad (7)$$

for some $\delta > 0$. The condition $P_{22} = 0$ therefore requires that $\text{tr}(|v_i\rangle\langle v_i|\sigma_2) = 0, i \in \mathcal{I}$, and $\text{tr}(|u_i\rangle\langle u_i|\rho_2) = 0, i \notin \mathcal{I}$, so

$$M = \sum_{i\in\mathcal{I}} \lambda_i \rho_1^\perp \otimes \sigma_2^\perp + \sum_{i\notin\mathcal{I}} \lambda_i \rho_2^\perp \otimes \sigma_1^\perp. \quad (8)$$

Using this last decomposition, we get

$$\text{tr}(M\rho_3 \otimes \sigma_3) = \sum_{i\in\mathcal{I}} \lambda_i \text{tr}(\rho_1^\perp \rho_3)\text{tr}(\sigma_2^\perp \sigma_3)$$
$$+ \sum_{i\notin\mathcal{I}} \lambda_i \text{tr}(\rho_2^\perp \rho_3)\text{tr}(\sigma_1^\perp \sigma_3)$$
$$\geq \delta' \sum_{i=1}^K \lambda_i \geq \delta'\text{tr}(M\rho_1 \otimes \sigma_2) > 0. \quad (9)$$

with $\delta' > 0$. But $P_{33} = 0$, from which it follows that M is indeed entangling. Actually, it is possible to obtain a non-linear witness to detect M's entanglement if we just follow the previous steps carefully while keeping track of the approximation errors (see the Appendix).

We have thus proven that $P \notin \tilde{P}^{unent}$, i.e., the matrix of probabilities P cannot be observed if only unentangled

measurements are allowed. However, the matrix P_{xy} can be expressed as a convex combination of four deterministic classical strategies. Indeed,

$$P = \frac{1}{4}\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \frac{1}{4}\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} + \frac{1}{4}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} + \frac{1}{4}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \quad (10)$$

The sets $\tilde{P}^C, \tilde{P}^{LOCC}, \tilde{P}^{unent}$ are hence not convex, since otherwise P would belong to them. Allowing the three parties to have shared randomness thus leads to a radically different scenario.

IV. NUMERICAL STUDY OF P^C, P^{unent} AND P^{ent} IN THE $N22$ SCENARIO

A. Procedure

Since convex sets can be completely characterized by systems of linear inequalities, it is legitimate to investigate how different linear constraints on P^C of the form $\sum_{x,y} W_{xy}P_{xy} \leq w_c$ may be violated by elements of P^{unent} and P^{ent}.

This leads us to the problem of maximizing quantities like

$$\sum_{x,y=1}^N W_{x,y}P_{x,y} = \sum_{x,y=1}^N W_{xy}\text{tr}(\rho_x \otimes \sigma_y M) \quad (11)$$

over all possible POVM elements M in the unentangled or the general class, and over all qubit states ρ_x and σ_y so as to get the values w_{unent} and w_{ent}. Clearly, if $w_{ent} > w_{unent}$ for some matrix W, then there exist experimental situations where one can prove that the statistics observed in the lab cannot be simulated with unentangled measurements and shared randomness.

Numerical optimization to obtain w_{unent} is carried out very similarly to the iterative algorithm used in [14]. The steps are the following:

1. Generate some random pure qubit states ρ_x, σ_y, $x, y = 1, 2, \ldots, N$.

2. In dimension $D = 2$, for fixed states ρ_x, σ_y, maximizing Eq. (11) reduces to a semidefinite problem: define thus $F \equiv \sum_{x,y=1}^N W_{x,y}\rho_x \otimes \sigma_y$, and maximize $\text{tr}(MF)$, subject to $M \succeq 0, \mathbb{1} - M \succeq 0, PT(M) \succeq 0, \mathbb{1} - PT(M) \succeq 0$, where PT denotes Partial Transposition [12, 13].

3. Fix M and σ_y and maximize $\text{tr}(G_x\rho_x) = \langle\psi_x|G_x|\psi_x\rangle$ for $x = 1, 2, \ldots, N$ where $G_x = \text{tr}_B(\sum_y \mathbb{1} \otimes \sigma_y M)$. This amounts to find the maximum eigenvalue of G_x with the corresponding eigenvector $|\psi_x\rangle$ for each x.

4. For fixed M and ρ_x, the optimal σ_y can be found such as ρ_x in step 3.

5. If convergence has not been achieved, go back to step 2.

This optimization algorithm may encounter several local optima, therefore we must iterate it many times in order to ascertain with reasonable confidence that the largest maximum has been found. In Sections IV B and IV C the semidefinite programs described in step 2 were solved using the SeDuMi package [15].

A very similar procedure can be applied if we wish to inquire about the maximal value w_{ent} which can be achieved within the class of general quantum measurements. The only difference is in step 2, where we have to maximize $\text{tr}(MF)$ subject to the only constraint $0 \preceq M \preceq \mathbb{1}$. However, in this case the maximum for a fixed F can be easily found by diagonalization $F = \sum_{i=1}^{4} \lambda_i |\phi_i\rangle\langle\phi_i|$, resulting in the optimal $M = \sum_{i=1}^{4} \frac{\text{sgn}(\lambda_i)+1}{2} |\phi_i\rangle\langle\phi_i|$. Thereby the optimization algorithm for the case of entangled measurements is much faster.

B. The 322 scenario

We next describe the way linear witnesses were produced for entangled measurements. Our starting point is the classical polytope P^C for the 322 scenario, consisting of 104 extremal points in dimension 9. All its facets can be enumerated by using the double description method implemented in Fukuda's cdd package [16]. The polytope P^C has 1230 facets; among them, 9 describe positivity facets $P_{x,y} \geq 0$, $x,y = 1,2,3$. The rest of them define non-trivial inequalities W. However, most of them are equivalent under the following operations,

- permuting Alice's inputs x

- permuting Bob's inputs y

- exchanging parties Alice and Bob

- multiplying by -1 all coefficients $W_{x,y}$ of the matrix W.

It turns out that there are 13 inequivalent facets of the polytope P^C. Those are listed in Table I, where we also give the maximum classical value w_c, the value w_{unent} achievable with unentangled measurements, the value w_{ent} attainable with general measurements, and the number of vertices lying on the particular facet. We must stress that the values for w_{unent} and w_{ent} come from numerical optimization, and so only local optimality is guaranteed. Nevertheless, due to the small dimensionality of the problem and the number of iterations of the main algorithm, we are quite confident about their overall optimality as well. Interestingly, we found that in each of the 13 cases w_{unent} could be achieved with rank-2 projective measurement operators.

We now focus on inequality #4 from Table I, which is the only inequality for which $w_{ent} > w_{unent}$, and hence

it enables to witness entangled measurements. The inequality looks (in an equivalent form) as

$$- P_{11} - P_{12} + P_{13} + P_{21} + P_{23} + P_{31} - P_{32} - P_{33}$$
$$\leq \frac{2 + 3\sqrt{6}}{4} \simeq 2.3371, \tag{12}$$

and can be violated by entangled measurements up to the value of 2.5. Next, we present the actual measurements and states achieving w_{ent} and w_{unent}.

Entangled case. The POVM element M is a rank-2 projector

$$M = |m\rangle\langle m| + |m^\perp\rangle\langle m^\perp|, \tag{13}$$

with

$$|m\rangle = (0, \cos\theta, \sin\theta, 0)$$
$$|m^\perp\rangle = \left(\frac{\cos\phi}{\sqrt{2}}, -\sin\phi\sin\theta, \sin\phi\cos\theta, -\frac{\cos\phi}{\sqrt{2}}\right), \tag{14}$$

having $\theta = 2\arctan(\frac{\sqrt{10}-1}{3})$ and $\phi = \pi/3$. The partial transpose of M has the following eigenvalues:

$$\lambda = \left(\frac{5-\sqrt{41}}{10}, \frac{1}{5}, \frac{4}{5}, \frac{5+\sqrt{41}}{10}\right), \tag{15}$$

with the first entry being negative. Both Alice's and Bob's states are pure and real valued, $\rho_x = |\psi_x\rangle\langle\psi_x|$ and $\sigma_y = |\phi_y\rangle\langle\phi_y|$, respectively. Their explicit forms are, respectively,

$$|\psi_1\rangle = (1, 0),$$
$$|\psi_2\rangle = (\cos\alpha, \sin\alpha),$$
$$|\psi_3\rangle = (\cos 2\alpha, \sin 2\alpha),$$

and $|\phi_y\rangle = |\psi_y\rangle$ for $y = 1, 2, 3$ with $\alpha = 2\arctan\left(\frac{2\sqrt{10}-\sqrt{15}}{5}\right) \simeq 0.9117$ rad. With these values in hand, the probability matrix P with components $P_{x,y} = \text{tr}(\rho_x \otimes \rho_y M)$ looks as follows:

$$P = \begin{pmatrix} 0.125 & 0.25 & 0.875 \\ 0.25 & 0.5 & 0.75 \\ 0.875 & 0.25 & 0.125 \end{pmatrix}. \tag{16}$$

And, indeed, evaluating the left-hand side of inequality (12), we get w_{ent}=2.5.

Unentangled case. In appropriate local bases, a separable rank-2 projective operator can be written in the form

$$M = |0\rangle\langle 0| \otimes |m\rangle\langle m| + |1\rangle\langle 1| \otimes |0\rangle\langle 0|, \tag{17}$$

where $|m\rangle = (\cos\theta, \sin\theta)$, and in our particular case, $\theta = \frac{1}{2}\arccos\frac{-1}{4} \simeq 0.911738$ rad. The states $\rho_x = |\psi_x\rangle\langle\psi_x|$ and $\sigma_y = |\phi_y\rangle\langle\phi_y|$, on the other hand, are given by

$$|\psi_1\rangle = (1, 0), \qquad |\phi_1\rangle = (1, 0),$$
$$|\psi_2\rangle = (1, 0), \qquad |\phi_2\rangle = (\cos\alpha, \sin\alpha),$$
$$|\psi_3\rangle = (0, 1), \qquad |\phi_3\rangle = (\cos -\alpha, \sin -\alpha), \tag{18}$$

TABLE I: Results for the 13 facet inducing inequalities in the 322-scenario.

Case	w_c	w_{unent}	w_{ent}	vertices	W_{11}	W_{12}	W_{13}	W_{21}	W_{22}	W_{23}	W_{31}	W_{32}	W_{33}
1	6	6.4006	6.4006	11	-2	-1	1	2	4	-2	4	-5	-1
2	2	2.8284	2.8284	13	-2	0	2	-2	1	-1	0	1	-1
3	1	1.4142	1.4142	20	-1	-1	0	0	1	0	1	-1	0
4	2	2.3371	2.5	16	-1	-1	0	-1	1	1	1	-1	1
5	1	1.3371	1.3371	12	-1	-1	1	-1	0	-1	0	1	0
6	2	2.6742	2.6742	10	-2	-1	2	-2	1	-1	0	1	0
7	2	2.1623	2.1623	9	-1	0	1	0	2	-2	1	-2	-1
8	2	2.1403	2.1403	10	-2	-1	1	0	2	-2	2	-3	-1
9	1	1.2058	1.2058	10	-1	-1	1	0	1	-1	1	-2	-1
10	2	2.7275	2.7275	14	-3	-2	1	-2	2	0	1	-1	1
11	1	1.3094	1.3094	16	-2	-2	1	-1	1	0	1	-1	0
12	3	3.8467	3.8467	11	-5	-3	2	-3	3	-1	2	-1	1
13	2	2.1186	2.1186	9	-3	-1	2	-1	2	-3	2	-3	-1

with $\alpha = -\arctan\left(\sqrt{\frac{8}{5}} + \sqrt{\frac{3}{5}}\right) \simeq -1.11493$ rad. With these, the probability vector is

$$P = \begin{pmatrix} 0.375 & P_{12} & P_{13} \\ 0.375 & P_{12} & P_{13} \\ 1 & P_{12} & P_{12} \end{pmatrix}, \qquad (19)$$

where $P_{12} = \frac{5}{4(4+\sqrt{6})} \simeq 0.193814$ and $P_{13} = \frac{P_{12}}{2}(5 + 2\sqrt{6}) \simeq 0.959279$. Plugging these numbers into the left-hand side of inequality (12), we get $w_{unent} = \frac{2+3\sqrt{6}}{4} \simeq 2.3371$. In some sense, the probability vector (19) approximates the best way among unentangled measurements the probability vector (16) corresponding to an entangled measurement.

C. The 422 scenario

The classical polytope P^C for the 422 scenario is spanned by 520 non-redundant vertices in the 16 dimensional probability space. However, it turned out that the full characterization of this polytope in terms of facets is computationally an elusive task. Instead, the problem was approached in a different way. We scanned through all the inequalities with small integer coefficients $(-1, 0, +1)$, and sorted out all of them which are facet defining. Several inequivalent facets have been found in this way (beyond the ones, which are just straightforward extensions of the 322-type inequalities in Table I). In Table II, we list all those 10 inequivalent facets for which $w_{ent} > w_{unent}$, hence witnessing entangled measurements. Among them, #9 is equivalent to the single 322-type witness in (12). Table II contains results on w_c, w_{unent}, w_{ent}, and also gives the sole negative eigenvalue λ_1 of $PT(M)$ achieving w_{ent}. Since all the other eigenvalues are positive, the absolute value $|\lambda_1|$ defines negativity, a valid entanglement measure [17].

Inequality #2 is interesting on its own. In this case, $w_{ent} = 3.3195$ is attained with a negativity of 0.1744, although a larger value of negativity of 0.1777 is found at another locally optimal point with $w'_{ent} = 3.145$. This feature resembles the dual case obtained in a Bell scenario, where for several tight 2-party Bell inequalities the maximum quantum value was achieved with non-maximally entangled 2-qubit states [18]. It has also been observed that for all the 422 witnesses for which unentangled measurements gave numerically maximal violation, the measurements could always be brought to a form of rank-2 projective matrices.

To conclude this section, the 422 scenario gave us a few new entangled measurement witnesses over the single witness of (12) of the 322 scenario. However, no significant improvement could be found in the efficiency of detecting entangled measurements with respect to unentangled measurements. Also, no simple generalization of inequality (12) for larger input alphabets was discovered among the 422 inequalities.

V. CONCLUSION

In this paper, we have studied how to translate the concept of witnessing entangled measurements to the device-independent arena. We found that even in a black-box scenario it is possible for a theorist to assert that a joint demolition measurement cannot be simulated with any sequence of local measurements assisted by classical communication: the only assumption one has to rely on is the dimensionality of the probe states. Following this line of thought, we derived correlation inequalities which allow to test the superiority of entangled measurements over unentangled ones in two-qubit experiments where 9 (Secs. III, IV B) and 16 correlation terms (Sec. IV C) are estimated.

Previous routes to certify the 'non-locality' of unknown

TABLE II: Results for the 10 facet inducing inequalities witnessing entangled measurements in the 422-scenario.

Case	w_c	w_{unent}	w_{ent}	vertices	λ_1	W_{11}	W_{12}	W_{13}	W_{14}	W_{21}	W_{22}	W_{23}	W_{24}	W_{31}	W_{32}	W_{33}	W_{34}	W_{41}	W_{42}	W_{43}	W_{44}
1	2	2.3371	2.3510	31	-0.1238	-1	-1	-1	0	-1	0	1	0	-1	1	-1	1	1	-1	0	1
2	3	3.2361	3.3195	34	-0.1744	-1	-1	-1	0	-1	0	1	1	0	1	-1	1	1	-1	0	1
3	2	2.3371	2.4369	38	-0.1154	-1	-1	-1	1	-1	0	1	-1	0	0	0	0	0	1	0	1
4	2	2.3371	2.4339	25	-0.1133	-1	-1	-1	1	-1	0	1	-1	0	0	1	1	1	-1	0	-1
5	1	1.3371	1.3413	28	-0.1016	-1	-1	0	0	-1	0	-1	0	0	0	0	1	0	1	-1	-1
6	2	2.3371	2.4322	24	-0.1089	-1	-1	0	0	-1	0	-1	1	0	1	-1	-1	1	0	0	1
7	2	2.1623	2.3028	19	-0.0718	-1	-1	0	0	-1	1	-1	1	1	0	-1	0	1	0	0	-1
8	2	2.1623	2.3028	26	-0.0718	-1	-1	0	0	-1	1	0	0	1	-1	-1	1	1	1	-1	-1
9	2	2.3371	2.5	72	-0.1403	-1	-1	0	0	-1	1	0	1	0	0	0	0	1	-1	0	1
10	2	2.2058	2.3773	22	-0.0982	-1	-1	0	0	-1	1	0	1	0	1	-1	-1	1	-1	-1	1

measuring devices involved carrying out complete tomography of their associated POVM elements [19], or envisaging a state discrimination problem where entangled measurements have an advantage with respect to unentangled ones [6, 8]. Either scheme has been conducted experimentally [19, 20] with success. Both approaches, though, relied crucially on a detailed knowledge of the probe states to be measured, and so their conclusions cannot be considered definite.

In contrast, in this article we have proven that the experimental inaccuracies arising from an imperfect preparation of the probe states can be completely eliminated by certifying entangled measurements within a black box approach. Given the simplicity of our inequalities, we thus propose their experimental implementation as an interesting challenge.

Appendix A: A Non-linear witness

In order to obtain a witness to certify the non-locality of P in Eq. (3), we will make use of the following result.

Proposition 1. Let $A \in B(\mathbb{C}^d)$ satisfy $0 \preceq A \preceq \mathbb{I}_d$, and let $\omega_1, \omega_2 \in B(\mathbb{C}^d)$ be two normalized quantum states, with $tr(A\omega_i) = P_i$, for $i = 1, 2$. Then,

$$tr(\omega_1 \cdot \omega_2) \leq (f(P_1, P_2))^2, \qquad (A1)$$

where

$$f(P_1, P_2) \equiv \sqrt{P_1 \cdot P_2} + \sqrt{(1 - P_1) \cdot (1 - P_2)}. \qquad (A2)$$

Moreover, there exist two states $\tilde{\omega}_1, \tilde{\omega}_2 \in B(\mathbb{C}^d)$ and a POVM element $\tilde{A} \in B(\mathbb{C}^d)$ that saturate the former inequality.

Proof. Let $\sum_i \mu_i |i\rangle\langle i|$ be the spectral decomposition of A, where $0 \leq \mu_i \leq 1$ and $\{|i\rangle\}_{i=0}^{d-1}$ is an orthonormal basis of $\mathbb{C}^d$. Then, Eq. (A1) follows from the next chain of inequalities:

$$(\mathrm{tr}\{\omega_1 \cdot \omega_2\})^{1/2} = \left(\sum_{i,j} \langle i|\omega_1|j\rangle\langle j|\omega_2|i\rangle\right)^{1/2} \leq \left(\sum_{i,j} (\langle i|\omega_1|i\rangle\langle j|\omega_1|j\rangle)^{1/2} (\langle i|\omega_2|i\rangle\langle j|\omega_2|j\rangle)^{1/2}\right)^{1/2} =$$

$$= \sum_i (\langle i|\omega_1|i\rangle\langle i|\omega_2|i\rangle)^{1/2} = \sum_i (\mu_i\langle i|\omega_1|i\rangle\mu_i\langle i|\omega_2|i\rangle)^{1/2} + \sum_i ((1-\mu_i)\langle i|\omega_1|i\rangle(1-\mu_i)\langle i|\omega_2|i\rangle)^{1/2} \leq$$

$$\leq \left(\sum_i \mu_i\langle i|\omega_1|i\rangle\right)^{1/2} \left(\sum_i \mu_i\langle i|\omega_2|i\rangle\right)^{1/2} + \left(\sum_i (1-\mu_i)\langle i|\omega_1|i\rangle\right)^{1/2} \left(\sum_i (1-\mu_i)\langle i|\omega_2|i\rangle\right)^{1/2} =$$

$$= \sqrt{P_1 \cdot P_2} + \sqrt{(1 - P_1) \cdot (1 - P_2)}. \qquad (A3)$$

To see that the bound is optimal, choose $A = |0\rangle\langle 0|$ and notice that the relations $|\langle\psi_{1,2}|0\rangle|^2 = P_{1,2}$ and $|\langle\psi_1|\psi_2\rangle|^2 = f(P_1, P_2)^2$ hold for the states $|\psi_{1,2}\rangle = \sqrt{P_{1,2}}|0\rangle + \sqrt{1 - P_{1,2}}|1\rangle$.

$\square$

Taking $A = M$ and $\omega_1 = \rho_j \otimes \sigma_l$ ($\omega_1 = \rho_l \otimes \sigma_j$), $\omega_2 = \rho_k \otimes \sigma_l$ ($\omega_2 = \rho_l \otimes \sigma_k$) in Proposition 1, it is easy to see that

$$\mathrm{tr}(\rho_j \cdot \rho_k) \ \leq \ \min_l f(P_{jl}, P_{kl})^2$$
$$(\mathrm{tr}(\sigma_j \cdot \sigma_k) \ \leq \ \min_l f(P_{lj}, P_{lk})^2). \qquad (A4)$$

These relations will play an important role when combined with the next proposition.

Proposition 2. *Let $\omega = \lambda |u\rangle\langle u| \otimes |v\rangle\langle v| \in B(\mathbb{C}^2 \otimes \mathbb{C}^2)$, with $\lambda > 0$, let $\{\rho_j, \sigma_j\}_{j=1}^3$ be normalized qubit states such that $\mathrm{tr}\{\rho_j \cdot \rho_k\}, \mathrm{tr}\{\sigma_j \cdot \sigma_k\} \leq C$, and let $\mathrm{tr}\{\omega \rho_j \otimes \sigma_j\} \leq c$. Then,*

$$\lambda \leq \frac{4c}{(1-\sqrt{C})^2}. \qquad (A5)$$

Proof. Let $\rho_j = \frac{\mathbb{I} + \vec{m}_j \cdot \vec{\sigma}}{2}$, $\sigma_j = \frac{\mathbb{I} + \vec{n}_j \cdot \vec{\sigma}}{2}$. By hypothesis we have that

$$(1 + \vec{u} \cdot \vec{m}_j) \cdot (1 + \vec{v} \cdot \vec{n}_j) \leq \tilde{c}, \qquad (A6)$$

for $j = 1, 2, 3$, where $\tilde{c} := 4c/\lambda$. It follows that, for each inequality j, at least one of the factors on the left-hand side is smaller or equal than $\sqrt{\tilde{c}}$. This implies that there exist two indices $j, k \in \{1, 2, 3\}, j \neq k$, such that either

$$(1 + \vec{u} \cdot \vec{m}_{j,k}) \leq \sqrt{\tilde{c}} \qquad (A7)$$

or

$$(1 + \vec{v} \cdot \vec{n}_{j,k}) \leq \sqrt{\tilde{c}} \qquad (A8)$$

holds. Let us assume that Eq. (A7) is true. Then we have that

$$\|\vec{m}_j + \vec{m}_k\| \geq -\vec{u} \cdot (\vec{m}_j + \vec{m}_k) \geq 2 - 2\sqrt{\tilde{c}}, \qquad (A9)$$

and hence

$$\lambda \leq \left(\frac{4\sqrt{c}}{2 - \|\vec{m}_j + \vec{m}_k\|} \right)^2. \qquad (A10)$$

On the other hand,

$$\|\vec{m}_j + \vec{m}_k\|^2 \leq 2(1 + \vec{m}_j \cdot \vec{m}_k) = 4\mathrm{tr}(\rho_j \cdot \rho_k) \leq 4C. \qquad (A11)$$

Combining Eqs. (A10) and (A11), we arrive at

$$\lambda \leq \frac{4c}{(1-\sqrt{C})^2}. \qquad (A12)$$

Had we supposed that Eq. (A8) were true, we would have obtained the same relation. Eq. (A5) then follows from the fact that at least one of the conditions (A7), (A8) must hold. $\qquad \square$

We are now ready to derive the non-linear inequality. Suppose that M is of the form

$$M = \sum_{i=1}^K \lambda_i |u_i\rangle\langle u_i| \otimes |v_i\rangle\langle v_i|, \qquad (A13)$$

with $\lambda_i > 0$. It is straightforward that the relation

$$\lambda_i \langle u_i|\rho_j|u_i\rangle\langle v_i|\sigma_j|v_i\rangle \leq c_i \equiv \lambda_i \sum_{k=1}^3 \langle u_i|\rho_k|u_i\rangle\langle v_i|\sigma_k|v_i\rangle \qquad (A14)$$

holds for $j = 1, 2, 3$. Also, notice that

$$\sum_i c_i = P_{11} + P_{22} + P_{33}. \qquad (A15)$$

Identifying $C = R^2$, with

$$R \equiv \max_{j \neq k} \left\{ \min_l f(P_{jl}, P_{kl}), \min_l f(P_{lj}, P_{lk}) \right\}, \qquad (A16)$$

in Proposition 2, we thus arrive at the bound $\lambda_i \leq \frac{4c_i}{(1-R)^2}$. Putting all together, we have that

$$\sum_{i=1}^K \lambda_i \leq \frac{4\sum_{i=1}^K c_i}{(1-R)^2} = \frac{4(P_{11} + P_{22} + P_{33})}{(1-R)^2}, \qquad (A17)$$

where in the last step we made use of Eq. (A15).

On the other hand,

$$\sum_i \lambda_i \geq \sum_i \lambda_i \mathrm{tr}(|u\rangle\langle u|\rho_k) \cdot \mathrm{tr}(|v\rangle\langle v|\sigma_l) = P_{kl}, \qquad (A18)$$

for all $k, l = 1, 2, 3$, and so the inequality

$$\frac{4(P_{11} + P_{22} + P_{33})}{(1-R)^2} - P_{k,l} \geq 0, \qquad (A19)$$

with R given by Eq. (A16), must hold for all k, l.

It is immediate to see that the example P in Section III violates it by an amount of $-1/4$.

[1] J.S. Bell, Physics **1**, 195 (1964).
[2] H. Buhrman, R. Cleve, S. Massar and R. de Wolf, Rev. Mod. Phys. **82**, 665 (2010).
[3] A. Acín et al., Phys. Rev. Lett. **98**, 230501 (2007); E. Hänggi, R. Renner, S. Wolf, arXiv:0911.4171v2 (2009); J. Silman et al., arXiv:1101.5086v2 (2011).
[4] S. Pironio et al., Nature **464**, 1021 (2010); R. Colbeck and A. Kent, arXiv:1011.4474v1 (2010).
[5] C.-E. Bardyn, T.C.H. Liew, S. Massar, M. McKague, and V. Scarani, Phys. Rev. A **80**, 062327 (2009); M. McKague, and M. Mosca, arXiv:1006.0150v1 (2010); Y.-C. Liang, T. Vértesi, N. Brunner, arXiv:1012.1513v1 (2010).

[6] A. Peres and W.K. Wootters, Phys. Rev. Lett. **66**, 1119 (1991).

[7] C.H. Bennett et al., Phys. Rev. A **59**, 1070 (1999).

[8] N. Gisin and S. Popescu, Phys. Rev. Lett. **83**, 432 (1999).

[9] C.H. Bennett and P.W. Shor, IEEE Trans. Info. Theory **44**, 2724 (1998).

[10] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).

[11] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett., **87**, 167902 (2001).

[12] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[13] M. Horodecki, P. Horodecki and R. Horodecki, Physics Letters A, **223**, 1 (1996).

[14] M. Navascués and T. Vértesi, arXiv:1010.5191 (2010).

[15] J. Sturm, SeDuMi, a MATLAB toolbox for optimization over symmetric cones, `http://sedumi.mcmaster.ca/`.

[16] K. Fukuda, `www.ifor.math.ethz.ch/~fukuda/cdd_home/`.

[17] O. Gühne and G. Tóth, Phys. Rep. **474**, 1 (2009).

[18] N. Brunner and N. Gisin, Phys. Lett. A **372**, 3162 (2008); K.F. Pál and T. Vértesi, Phys. Rev. A **79**, 022120 (2009).

[19] J.S. Lundeen et al., Nature Physics 5, 27 (2009).

[20] G.J. Pryde et al., Phys. Rev. Lett. **94**, 220406 (2005); E.R. Jeffrey et al., Phys. Rev. Lett. **96**, 150503 (2006); J. Niset et al., Phys. Rev. Lett. **98**, 260404 (2007).